

DÖKSAN ISIL İŞLEM A.Ş.
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

I. GİRİŞ

1.1. AMAÇ

İşbu Kişisel Veri Saklama ve İmha Politikası ("**Politika**"), veri sorumlusu olarak Döksan Isıl İşlem A.Ş. ("**Döksan**" veya "**Şirket**") tarafından, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**Kanun**") ve Kişisel Verileri Koruma Kurumu ("**Kurum**") tarafından 28/10/2017 tarihli ve 30224 sayılı Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("**Yönetmelik**") ilgili hükümleri uyarınca, veri saklama ve imha faaliyetlerine ilişkin olarak usul ve esasları belirlemek amacıyla hazırlanmıştır.

Bu kapsamda Politika, mevzuattan doğan yükümlülüklerimizi yerine getirerek, Şirket çalışanlarımızın, çalışan adaylarımızın, müşterilerimizin ve sair nedenler ile Döksan bünyesinde kişisel verileri bulunan tüm gerçek kişi veri sahiplerinin haklarını etkin bir şekilde kullanmasına olanak tanımak amacıyla hazırlanmış olup, verilerin saklanmasına ve imhasına ilişkin tüm iş ve işlemler işbu Politikaya uygun olarak gerçekleştirilecektir.

1.2. TANIMLAR

Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

Alıcı grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,

Anonim hale getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,

Elektronik ortam: Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamları,

Elektronik olmayan ortam: Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamları,

İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

İlgili kullanıcı: Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri,

İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,

Kanun: 24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanununu,

Kayıt ortamı: Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı,

Kurul: Kişisel Verileri Koruma Kurulunu,

Periyodik imha: Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini,

Politika: Kişisel Verileri Saklama ve İmha Politikasını,

Sicil: Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini,

Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,

Yönetmelik: 28.10.2017 tarihli ve 30224 sayılı Resmi Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği, ifade eder.

II. KİŞİSEL VERİLERİ SAKLAMA ORTAMLARI

Döksan nezdinde bulunan kişisel veriler, verilerin niteliğine ve mevzuattan doğan hukuksal yükümlülöklere uygun olarak ve gerekli güvenlik önlemleri alınmak şartıyla saklanmaktadır.

Kişisel verilerin saklama ortamları aşağıda belirtildiği gibidir;

Elektronik Olmayan Ortamlar	Elektronik Ortamlar
- Kağıtlar ve mikrofiş ortamları	- Yazılımlar (Ofis yazılımları vb.)
- Yazılı, basılı ve görsel ortamlar	- Bilgisayarlar, telefonlar, tabletler
	- Optik diskler (CD, DVD vb.)
	- Taşınabilir bellekler (Hafıza kartı, USB, Hard disk vb.)
	- Bulut ortamları (Office 365, Dropbox vb.)

III. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

3.1. SAKLAMA SEBEPLERİ

Kişisel verilerin işlenmesi ve bu cihetle saklanmasını gerektiren sebepler, www.doksanisilislem.com adresinde bulunan Aydınlatma Metni'nde sayma yöntemiyle açıklanmıştır.

Veri sahiplerine ilişkin kişisel veriler; (ı) kanunlarda açıkça öngörülmesi, (ıı) bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, (ııı) veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi, (ıv) bir hakkın tesisi, kullanılması veya korunması ve (v) ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri hukuki şartları çerçevesinde; ticari faaliyetlerin yürütülebilmesi, hukuki ve sözleşmesel yükümlülüklerin yerine getirilebilmesi ve müşteri ilişkilerinin yönetilebilmesi amacıyla yukarıda sayılan elektronik olmayan yahut elektronik ortamlarda güvenli bir biçimde mevzuatta belirtilen sınırlar çerçevesinde saklanmaktadır.

3.2. İMHA SEBEPLERİ

Kişisel veriler; aşağıdaki durumlarında, Şirket tarafından re'sen yahut ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir:

- İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilga edilmesi,
- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- Kanunun 11. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi,
- Şirketin, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

IV. İMHA YÖNTEMLERİ

Beyaz, Kanuna ve sair mevzuata uygun olarak sakladığı kişisel verileri, ilgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda, re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edecektir:

4.1. KİŞİSEL VERİLERİN SİLİNMESİ

Kişisel veriler, aşağıdaki tabloda belirtilen yöntemlerle silinir.

Veri kayıt ortamı	Açıklama
Kağıt Ortamında Bulunan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi,

	ilgili evrak üzerindeki kişisel verilerin kesilmesi, geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılır.
Hizmet Olarak Uygulama Türü Bulut Çözümleri (Office 365, Dropbox gibi)	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veritabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Bulut sisteminde veriler, silme komutu verilerek, ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisi olmaksızın silinir.
Sunucular	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.
Veri Tabanları	Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (Delete vb.) ve ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilerek silinir.
Merkezi Sunucuda Yer Alan Ofis Dosyaları	Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilir.

4.2. KİŞİSEL VERİLERİN YOK EDİLMESİ

Kişisel veriler, aşağıdaki tabloda belirtilen yöntemlerle yok edilir.

Veri kayıt ortamı	Açıklama
Yerel Sistemler	<p>i) De-manyetize Etme: Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerinde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.</p> <p>ii) Fiziksel Yok Etme: Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da</p>

	fiziksel olarak yok edilmesi gerekir. iii) Üzerine Yazma: Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.
Optik / Manyetik Medya	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerlerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.
Kağıt ve Mikrofiş Ortamları	Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan, kağıt imha veya kırpma makinaları ile anlaşılabilir boyutta ve geri birleştirilemeyecek şekilde küçük parçalara bölünür. Orijinal kağıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise buldukları elektronik ortama göre "Yerel Sistemler" başlığında belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.
Bulut Ortamı	Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenir ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılır. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılabilir hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir.

4.3. KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup/kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir. Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler, anonim hale getirilmiş veri sayılır.

Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri aşağıdaki gibidir:

Yöntem	Açıklama
Değişkenleri Çıkartma	İlgili kişiyi tespit etmeye yarayacak değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir. Böyle bir durumda tablodaki bütün sütun tamamıyla kaldırılacaktır.
Kayıtları Çıkartma	Veri kümesinde yer alan tekillik ihtiva eden bir satırın çıkartılması ile anonimlik kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür.

Bölgesel Gizleme	Belli bir kayda ait değerlerin yarattığı kombinasyon çok az görülebilir bir durum yaratırsa ve bu durum o kişinin ilgili toplulukta ayırt edilebilir hale gelmesine yüksek olasılıkla sebep olabileceksa istisnai durumu yaratan değer “bilinmiyor” olarak değiştirilir.
Genelleştirme	İlgili kişisel veriyi özel bir değerden daha genel bir değere çevirme işlemidir. Kümülatif raporlar üretirken ve toplam rakamlar üzerinden yürütülen operasyonlarda en çok kullanılan yöntemdir.
Alt ve Üst Sınır Kodlama	Belli bir değişken için bir kategori tanımlayarak bu kategorinin yarattığı gruplama içinde kalan değerleri birleştirerek elde edilir. Genellikle belli bir değişkendeki değerlerin düşük veya yüksek olanları bir araya toplanır ve bu değerlere yeni bir tanımlama yapılarak ilerlenir.
Global Kodlama	Alt ve üst sınır kodlamanın uygulanması mümkün olmayan, sayısal değerler içermeyen veya numerik olarak sıralanamayan değerlere sahip veri kümelerinde kullanılan bir gruplama yöntemidir. Genelde belli değerlerin öbeklenerek tahmin ve varsayımlar yürütmeyi kolaylaştırdığı hallerde kullanılır. Seçilen değerler için ortak ve yeni bir grup oluşturularak veri kümesindeki tüm kayıtlar bu yeni tanım ile değiştirilir.
Örnekleme	Örnekleme yönteminde bütün veri kümesi yerine, kümeden alınan bir alt küme açıklanır veya paylaşılır. Böylelikle bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da paylaşılan örnek alt küme içinde yer alıp almadığı bilinmediği için kişilere dair isabetli tahmin üretme riski düşürülmüş olur.

Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri aşağıdaki gibidir:

Yöntem	Açıklama
Mikro Birleştirme	Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Böylece o değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir.
Veri Değiş Tokuşu	Veri değiş tokuşu yöntemi, kayıtlar içinden seçilen çiftlerin arasındaki bir değişken alt kümeyle ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve ana fikir değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirerek veri tabanının dönüştürülmesidir.
Gürültü Ekleme	Bu yöntem ile, seçilen bir değişkende belirlenen ölçüde bozulmalar sağlamak için ekleme ve çıkartmalar yapılır.Bozulma her değerde eşit ölçüde uygulanır.

Döksan, kişisel verilerin anonim hale getirilmesi için ilgili verinin niteliğine göre yukarıda sayılan yöntemlerden bir ya da birkaçını kullanır. Döksan, bu anonimleştirme yöntemlerini kullanırken K-Anonimlik, L-Çeşitlilik ve T-Yakınlık istatistik yöntemlerini kullanabilir.

V. SAKLAMA VE İMHA SÜRELERİ

Şirket tarafından işlenen verilere ait saklama ve imha süreleri Kişisel Veri İşleme Envanterinde süreç bazında tespit edilmiş olup, anılan Envanter'e www.verbis.kvkk.gov.tr adresi üzerinden Sicil Sorgulama Ekranı Döksan aratılarak erişilebilecektir.

Süreç	Saklama Süresi	İmha Süresi

VI. SORUMLULUK VE GÖREV DAĞILIMLARI

Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi, izlenmesi ve denetimi, süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimler, yetkilileri ve görev tanımları aşağıdaki tabloda gösterilmiştir:

Unvan	Birim	Görev
İnsan Kaynakları Müdürü	İnsan Kaynakları Departmanı	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Bilgi İşlem Müdürü	Bilgi Teknolojileri Departmanı	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Muhasebe Müdürü	Mali İşler Departmanı	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin

		yönetimi
İdari İşler Müdürü	Veri Sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi

VII. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin saklandığı ortamların, ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak, teknik ve idari tedbirler alınır.

7.1. Teknik Tedbirler

- Kişisel verilerin saklandığı ortamlara yönelik risk, tehdit veya zafiyetleri önlemek amacıyla sızma testleri gerçekleştirilir.
- Kişisel veriler, güncel ve uygun teknolojik ortamlarda saklanır.
- Kişisel verilerin tutulduğu ortamlara yönelik güvenlik sistemleri kullanılır.
- Bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınır.
- Silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirler alınır.

7.2. İdari Tedbirler

- Çalışanların, kişisel verilerin gizliliği konusunda bilinçlendirilmesi amacıyla çalışmalar yapılır.
- Kişisel verileri erişim, yalnızca ilgili kullanıcı ile sınırlandırılır.
- Kişisel verilerin işlenmeye başlanılmasından önce aydınlatma yükümlülüğü yerine getirilir ve açık rıza gereken hallerde ilgili kişilerin rızası alınır.
- Kişisel verilere dışarıdan izinsiz erişim sağlanması halinde, durum gecikmeksizin Kuruma bildirilir.

VIII. PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11. maddesi gereğince Şirket, periyodik imha süresini 6 ay olarak belirlemiştir. Buna göre, Şirkette her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

IX. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır. Basılı kâğıt nüshası da ... dosyasında saklanır.

X. POLİTİKA'NIN GÜNCELLENME PERİYODU

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

XI. POLİTİKA'NIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, Şirketin internet sitesinde yayınlandığı tarih itibarıyla yürürlüğe girer. Politikanın yürürlükten kaldırılmasına karar verilmesi halinde, ıslak imzalı eski nüshaları Kurul Kararı ile ... tarafından iptal edilerek imzalanır ve en az 5 yıl süre ile ... tarafından saklanır.